REMARKS

Applicants respectfully requests reconsideration and allowance of subject application. Claims 1-2, 4-17, 19-27, 29-35, 38-41, 43-50, 52-58, and 60-61 were pending at the time of the Action. Claims 1, 10, 12, 16, 24, 26, 31, 38, 40, 49, and 58 are amended. Claims 1-2, 4-17, 19-27, 29-35, 38-41, 43-50, 52-58, and 60-61 remain pending.

Applicants appreciate the Examiner taking the time to speak with their attorney regarding the Office Action.

Claim Rejections under 35 U.S.C. § 102

Claims 1-2, 4-17, 19-27, 29-35, 38-41, 43-46, 48-55, 57-58, and 60-61 are rejected under 35 U.S.C. § 102 as being anticipated by Fox et al., "Security on the Move: Indirect Authentication Using Kerberos" (1996) (hereinafter "Fox"). Applicants respectfully traverse the rejection.

In the interest of reducing the number of issues for the Examiner to consider in this response, the following discussion focuses on independent Claims 1, 12, 16, 26, 31, 38, 40, 49, and 58. The patentability of each remaining dependent claim is not necessarily separately addressed in detail. However, applicants' decision not to discuss the differences between the cited art and each dependent claim should not be considered as an admission that applicants concur with the Examiner's conclusion that these dependent claims are not patentable over the disclosure in the cited references. Similarly, applicants' decision not to discuss differences between the prior art and every claim element, or every comment made by the Examiner, should not be considered as an admission that applicants concur with the Examiner's interpretation and assertions regarding those claims. Indeed, applicants believe that all of the dependent claims patentably distinguish over the references cited. Moreover, a specific traverse of the rejection of each dependent claim is not required, since dependent claims are patentable for at least the same reasons as the independent claims from which the dependent claims ultimately depend.

By way of introducing the context in which the invention was made and some of the problems which it addresses, the specification of the subject application addresses the problem of unconstrained forward target delegation. Generally, the user logon for a computer and the user

authentication for network access control are two separate procedures. Nevertheless, to minimize the burden on a user in dealing with the different access control schemes, the user logon and the user authentication for network access are sometimes performed together. For example, in the case where the user authentication is implemented under the Kerberos protocol, when the user logs on the computer, the computer may also initiate a Kerberos authentication process. In the authentication process, the computer contacts a Kerberos Key Distribution Center (KDC) to first obtain a ticket-granting ticket (TGT) for the user. The computer can then use the TGT to obtain from the KDC, a session ticket for itself.

As networks have evolved, there has been a trend to have multiple tiers of server/service computers arranged to handle client computer requests. A simple example is a client computer making a request to a World Wide Web website via the Internet. Here, there may be a front-end web server that handles the formatting and associated business rules of the request, and a back-end server that manages a database for the website. For additional security, the web site may be configured such that an authentication protocol forwards (or delegates) credentials, such as, e.g., the user's TGT, and/or possibly other information from the front-end server to a back-end server. This practice is becoming increasingly common in many websites, and/or other multiple-tiered networks.

Thus, any server/computer in possession of the user's TGT and associated authenticator can request tickets on behalf of the user/client from the KDC. This capability is currently used to provide forwarded ticket delegation. Unfortunately, such delegation to a server is essentially unconstrained for the life of the TGT.

With this in mind, methods and systems are provided to constrain or otherwise better control the delegation process. The methods and systems can be used with different authentication protocols. The delegation process is controlled in certain exemplary implementations through a service-for-user-to-proxy (S4U2proxy) technique. The S4U2proxy technique is preferably implemented as a protocol that allows a server or service, such as, e.g., a front-end server/service, to request service tickets on behalf of a client for use with other servers/services. As described in greater detail below, the S4U2proxy protocol advantageously provides for constrained delegation in a controllable manner that does not require the client to forward a TGT to the front-end server.

With the utmost respect for the Office Action and the Examiner, the concern recited in the specification of the present application with regard to unconstrained delegation is the same problem that is expressly conceded Fox and its description of "Charon, a proxied implementation of Kerberos." (Fox, Section 1.3, Page 155, Column 2, Paragraph 1). As cited by the Office Action, this proxied implementation not only allows, but supports, unconstrained delegation:

> An alternative approach to service access that places ***more trust in Charon*** is for the client to reveal $K_{c,tgs}$ to Charon over the established secure channel, thus allowing Charon to negotiate for Kerberized services directly."

(Fox, Section 2.3, Page 158, Column 2, Paragraph 3; emphasis added). As explained by Fox, "$K_{c,tgs}$" is a key generated by a key distribution center and disclosed to the principals "x and y," which in the case of "$K_{c,tgs}$" would be the client, c, and the Kerberos ticket-granting server. (Fox, Page 157, Column 2, Section 2.2, Paragraphs 3, 8, and 12). Thus, the passage cited by the Office Action expressly contemplates exposing the key disclosed to the client and the ticket-granting service to the proxy, Charon. Thus, the passage of the cited reference relied upon by the Office Action expressly allows for unconstrained delegation.

Not only does this passage of Fox allow for unconstrained delegation, but later in the same paragraph, Fox expressly concedes what a significant problem unconstrained delegation presents:

> "In this approach, Charon still doesn't have the user's Kerberos password, ***but because it has $K_{c,tgs}$, it can do more damage should it be comprised. Specifically an attacker who controls $K_{c,tgs}$ can impersonate the client for the lifetime of the TGT, requesting additional services that the client has not authorized. The ticket lifetime, which is specified at the time the TGT is requested, may be as lengthy as several hours, which presents a potentially large window during which attackers could cause damage.*** This second approach potentially increases convenience to the user at the cost of decreased security."

(Fox, Section 2.3, Page 158, Column 2, Paragraph 3 through Page 159, Column 1, Paragraph 1; emphasis added). Clearly, Fox's Charon system considers and tolerates a problem what was both recognized and discussed in the specification of the present application.

Applicants wish to note that, the "first approach" of Fox, described in Section 2.3, Page 158, Column 2, Paragraph 2, describes a process wherein neither the Charon password nor $K_{c,tgs}$, are provided by the client to the server; however, a session key is provided by the client to the proxy, allowing the proxy to operate on the client's behalf. Thus, in both approaches described

by Fox, a client expressly provides to a proxy or server a client authentication, which the proxy or server then can put to its own use.

By contrast, for example, what is recited in claim 1 is distinct from what is recited by Fox:

> 1. (Currently Amended) A method for constraining a scope of delegation by a client to a server, comprising:
>
> identifying a target service to which access is sought on behalf of a client;
>
> causing a server operatively coupled to the client to request access to the target service on behalf of the client, from a trusted third-party, wherein the server provides the trusted third-party with a credential authenticating the server, information about the target service, and a service credential previously provided by the client to the server; and
>
> causing the trusted third-party to provide the server with a new service credential granted in the name of the client rather than the server such that the new service credential authorizes the server to access the service on behalf of the client while withholding a client's authentication credentials from the server, wherein the new service credential granted in the name of the client is constrained to a scope specified by the service credential previously provided by the client to the server.

Respectfully, Fox teaches exposing client authentication credentials to a proxy or server, leading to the possibility of unconstrained delegation. By contrast, claim 1 as amended expressly recites constraining the scope of delegation by withholding the client's authentication credentials from the server. Fox fails to teach or suggest what is recited by claim 1. Thus, Claim 1 is not anticipated by Fox.

Independent claims 12, 16, 31, 38, 40, and 58 also are currently amended to recite methods and systems of constrained delegation that limit the scope of access permitted to a server to that scope permitted by a client. Accordingly, for reasons analogous to those submitted above with respect to Fox, applicants submit that claims 12, 16, 31, 38, 40, 49, and 58 are not anticipated by Fox.

Claim 26, as amended, further distinguishes over the reference cited. Specifically, claim 26 recites "presenting a forwardable delegation flag indicating the client has authorized the delegation." Applicants respectfully note that the Office Action does not expressly reference such an element. The Office Action mentions, without citation, that "Verifying authorized delegation is inherently implied in a system that uses Kerberos." However, the Office Action does not specify or cite authority for the proposition that such verification is so inherently

implied. Moreover, the Office Action's reliance on such an implication certainly fails to recite a mechanism by which such authentication is made. Thus, the "presenting of a forwardable flag" is neither mentioned nor even contemplated by the cited reference. Therefore, applicants submit that claim 26 as amended further distinguishes over the reference cited.

Claims 2, 4-11, 13-15, 17, 19-25, 27, 29-30, 32-35, 39-41, 43-46, 48, 50, 52-55, 57, and 60-61 are dependent claims that depend from and apply additional limitations to the claims from which each depends. Thus, each of claims 2, 4-11, 13-15, 17, 19-25, 27, 29-30, 32-35, 39-41, 43-46, 48, 50, 52-55, 57, and 60-61 is also patentable for at least the same reasons as the independent claim from which it depends.

Claim Rejections under 35 U.S.C. § 103

Claims 47 and 56 once again rejected under 35 U.S.C. § 103(a) as being obvious over Fox in view of Freier et al., "The SSL Protocol Version 3.0" (November 18, 1996). Claims 47 and 56 depend from claims 40 and 59, respectively. Because dependent claims 47 and 56 are patentable for at least the same reasons as the claims from which they depend, and add additional limitations to those claims, applicants request that the rejection similarly be withdrawn from claims 47 and 56.

CONCLUSION

Claims 1-2, 4-17, 19-27, 29-36, 38-41, 43-50, 52-58, and 60-61 are in condition for allowance. Applicant respectfully requests entry of the amendment, and reconsideration and prompt allowance of the subject application. If any issue remains unresolved that would prevent allowance of this case, the Examiner is requested to contact the undersigned attorney to resolve the issue.

Respectfully submitted,

MERCHANT & GOULD P.C.
P.O. Box 2903
Minneapolis, Minnesota 55402-0903
(206) 342-6200

Date: September 19, 2006

Frank J. Bozzo
Reg. No. 36,756
Direct Dial: (206) 342-6294